PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/08, 19/00	A1	(11) International Publication Number: **WO 97/02547** (43) International Publication Date: 23 January 1997 (23.01.97)

(21) International Application Number: PCT/EP96/02997

(22) International Filing Date: 5 July 1996 (05.07.96)

(30) Priority Data:
1000741 6 July 1995 (06.07.95) NL

(71) Applicant: KONINKLIJKE PTT NEDERLAND N.V. [NL/NL]; 7 Stationsplein, NL-9726 AE Groningen (NL).

(72) Inventor: DE ROOIJ, Peter, Jacobus, Nicolaas; Wijnpersstraat 30/13, B-3000 Leuven (BE).

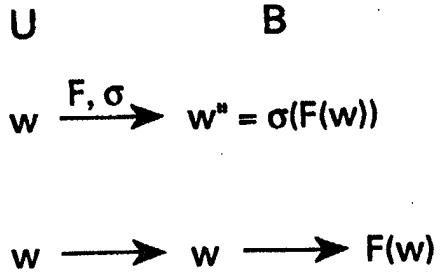
(81) Designated States: AU, BG, BR, CA, CN, CZ, EE, FI, HU, IL, JP, KR, LT, LV, MX, NO, NZ, PL, RO, SG, TR, UA, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR TRACING PAYMENT DATA IN AN ANONYMOUS PAYMENT SYSTEM, AS WELL AS PAYMENT SYSTEM IN WHICH THE METHOD IS APPLIED

(57) Abstract

The invention relates to a method for tracing payment data in an anonymous payment system having electronic payment means, such as so-called "smart cards". According to the invention, the user (U) commits himself to a value (w; w'') which may later be used for the tracing by a payment institution (B). The value (w) is preferably recorded with the help of a so-called one-way function (F) and an (electronic) signature (σ), so that the payment institution does not dispose of the value itself, but is able to verify it on the basis of the stored derivative (w'') of the value. The invention further relates to a payment means and a payment system for application of the method.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

Method for tracing payment data in an anonymous payment system, as well as payment system in which the method is applied.

BACKGROUND OF THE INVENTION

The invention relates to a method for tracing payment data in an anonymous payment system. More in particular, the invention relates to such method in the event that payment data have been lost due to damage of the payment means or premature interruption of a transaction.

In electronic payment systems, problems may arise if a payment means, such as a payment card, is damaged or lost. Particularly in the event of payment systems with payment in advance ("prepaid payment systems"), the value stored in the payment means may then be lost. In order in such case not to put the user at a disadvantage, the payment transactions effected should be reconstructed or at least traced, in order as yet to have a fair settlement take place of the actually effected payments.

Even if a (payment) transaction is prematurely broken off, payment data may be lost, with possible adverse consequences for the user of the payment means and/or for the receiver of the payment. In this case, payment data should also be traced, in order to prevent or undo possible harm.

In the event of anonymous payment systems, i.e., payment systems in which the payments cannot afterwards be related to a certain user (payer), the problem arises that reconstructing or tracing effected payment transaction in most cases is impossible. It is specifically the anonymous nature of such payment systems which impedes transactions being traced. The users of such systems can therefore be harmed by the loss of, or damage to, their payment means.

Prior art documents, such as US Patents 5 018 196 and 4 993 068, or European Patent Applications 0 637 004 and 0 518 365, do not offer a solution to these problems. US Patent 5 018 196, for instance, deals with the exchange of digital signatures of contract documents through an information network. Preliminary digital signatures are exchanged between parties in order to provide evidence in case problems arise. The said Patent does not deal with the tracing of payment data in an anonymous payment system.

SUMMARY OF THE INVENTION

It is an object of the invention to eliminate the above and other drawbacks of the prior art and to provide a method which makes it possible, in an anonymous payment system, to trace transactions and, if necessary, to reconstruct these transactions, with the anonymity of the user being protected as much as possible.

It is a further object of the invention to provide a payment system in which the above-mentioned method is applied.

For this purpose, the invention provides a method for tracing payment data in an anonymous payment system having electronic payment means and at least one payment institution designed for electronic payments, which method comprises: a first step in which the user issues a value characterising his payment data to the payment institution, which value is stored by the payment institution and, if tracing is desired, a second step in which the user releases the value, whereafter payment data are checked on the basis of the said value.

The invention is based on the insight that, for tracing lost transactions, the anonymity of the payment system must be breached, at least in part. The invention is also based on the further insight that the anonymity be preferably breached only with the co-operation of the user.

Breaching the anonymity may take place by making available, to the payment institution, information which is used by the payment means to construct a recognisable part of the (future) payments. The payment institution may analogously reconstruct such recognisable parts of the payments afterwards.

A preferred embodiment of the invention is based on the insight that it suffices for the user to commit himself to a value by issuing check information related to such value. In the first step, therefore, a check digit of the said value is advantageously recorded, instead of the value itself, with the user supplying the value itself only in the second step, or at least giving permission to use the value itself.

Preferably, the said value is blocked in the first step in such a manner that the payment institution cannot apply the value without the co-operation of the user. As a result, the anonymity of the user is maintained. On the other hand, the user commits himself to the

said value by means of the check value, so that the value cannot be modified by the user.

The value is advantageously blocked, in the first step, with the help of a one-way function. By means of a one-way function, it may be achieved that the value can be checked afterwards, while the value itself cannot be determined by the payment institution. This provides a further protection of the anonymity of the user.

EXEMPLARY EMBODIMENTS

The invention will be explained in greater detail below with reference to the Figures.

FIG. 1 schematically shows an embodiment of the method according to the invention.

FIG. 2 schematically shows an example of the application of the method according to the invention.

The embodiment of the method according to the invention schematically shown in FIG. 1 comprises two steps. The first step, indicated by I, is preferably carried out regularly, i.e., at fixed points in time or after every n transactions ($n \geq 1$), e.g., in the event of charging a (prepaid) payment means and/or in the event of any contact with the payment institution in question. The second step, indicated by II, is carried out only if payment data were lost and must be traced afterwards.

In the first step (I), the user commits himself to a value w; in other words, the user makes a so-called "commitment" to the value w. The value w itself, e.g., is the value (status) of the random generator (RNG) of the payment means in question. The said committing may take place by subjecting the value w to a one-way function and the subsequent affixing of a signature to the result of the one-way function. The application of the one-way function (F) has the advantage that the payment institution (indicated by "Bank" in FIG.1, but institutions other than banks can also be envisaged) cannot determine w from the resulting value w' (where $w' = F(w)$, F being the one-way function), so that the anonymity of the user is maintained. The payment institution is able to check w', however, by also calculating w' from the value w provided later. This will be explained in greater detail below.

It will be understood that a one-way function F known per se

from cryptography has the property that the reciprocal (F^{-1}) cannot, or cannot viably, be calculated. In other words, $w' = F(w)$ may be simply calculated from w, but it is not viable from w' to reconstruct the original value $w = F^{-1}(w')$. As a result, the one-way function provides a further protection of the user.

Affixing a (digital) signature to w' has the advantage that it can be proven, by the payment institution, that a certain user has supplied the value w in question (or w', w''). Affixing a signature to the value w', resulting in the value w'', is carried out with a function σ, which may be a function known per se from cryptography. The value w'', where $w'' = \sigma(w') = \sigma(F(w))$, is stored by the payment institution.

In the second step (II), the user "opens" the value committed to. This "opening" takes place, e.g., by providing the value w to the payment institution, whereafter the payment institution can reconstruct w' as $w' = F(w)$ and subsequently verify the signature w'' on w'. The payment institution then verifies, on the basis of the values of w used in various transactions, which transactions have been carried out successfully. The opening may take place by informing the payment institution that a stored value w may be used.

A further check may be obtained if the user repeatedly provides values w'' (possibly: w') to the payment institution, and the payment institution stores the i-th value ($i \geq 1$), whilst the i-1 preceding values are applied by the user only to verify the correct application of F and σ.

In fact, the method according to the invention comprises two submethods, corresponding to the said two steps: the first step comprises a method for protectedly storing reconstruction data, with the second step comprising a method for reconstructing payment data on the basis of reconstruction data.

In FIG. 2, there is schematically, and by way of example, illustrated a further elaboration of the second step of the method according to the invention.

In the first step, the payment means of the user has issued a value $w'' = \sigma(F(w))$ which is related to the status of the random generator of the payment means of the user in question. If payments (in general: transactions) are to be traced or reconstructed because, e.g., a payment means was lost or a transaction was prematurely

terminated, the user gives permission, in the second step, to use the value w stored at the payment institution ("Bank" in FIG. 2). In the case shown, this occurs by the user (or the payment means of the user, as the case may be) transferring the value w (stored for this purpose in the payment means) to the payment institution. As a result, the payment institution is able to verify the stored value w'' by calculating w' (w' = F(w)) and checking the signature on w'.

At the payment institution, there have e.g. been received the electronic cheques Ch1, Ch2 and Ch5, represented by (c1, b1), (c2, b2) and (c5, b5) respectively. In this example, it is assumed that the cheque Ch3 was never issued and that the transaction with the cheque Ch4 was broken off (represented by X in FIG. 2) due to a technical failure. It should be noted that instead of cheques other types of electronic payments, e.g. electronic coins, may be used as well.

The payment information consists, inter alia, of an identification ci (c1, c2 or c5), which is related to the status of the said random generator at the time of the "writing out" of the respective cheque, and an amount bi (b1, b2, b5). On the basis of the value w, the successive values ci (i=1...5) are now generated anew by the payment institution. On the basis of the value ci, the cheques Ch1, Ch2 and Ch5 may be traced, i.e., recognized as cheques of the user in question. Since the beneficiary of the payment communicates the amount to the payment agency, the amounts b1, b2, b5 are known to the payment institution as well.

This embodiment of the method may be applied for indemnifying the user in the event of loss or technical failure. On the basis of recognised (traced) payments, the difference between the sum of the paid amounts and the balance of the payment means at the moment of issuing the (derivative of the) value (w'') may be repaid to the user.

In the event that a payment is broken off prematurely, the method according to the invention may be applied to detect whether indeed a interrupted transaction was involved. If this was not the case, the payment may be traced. Here, the first step of the method may possibly be dispensed with; the user may immediately release the value. The payment means may possibly provide additional information on transactions gone wrong or broken off.

A payment system in which the invention is applied comprises at least a payment institution (such as a bank, credit card company, or

possibly telecommunications company), payment stations (such as cash registers of sales points designed for that purpose) and users having payment means (such as payment cards, "smart cards"). During a payment transaction, there is basically no direct connection required between a payment station and a payment institution. Such connection is advantageously set up only periodically, in order to settle transactions effected.

On the basis of the tracing of transactions according to the invention, i.e., the verification whether the transactions in question have taken place, the transactions effected may possibly be reconstructed as well. The payment transactions discussed above may take place with so-called electronic cheques.

It will be understood by those skilled in the art that the invention is not limited to the embodiments discussed above, and that many modifications and additions are possible without departing from the scope of the present invention.

CLAIMS

1. Method for tracing payment data in an anonymous payment system having electronic payment means and at least one payment institution (B) designed for electronic payments, which method comprises:

- a first step (I), wherein the user (U) issues a value (w) characterising his payment data to the payment institution, which value (w) is stored by the payment institution (B),

and, if tracing is desired,

- a second step (II), wherein the user (U) releases the value (w), whereafter payment data are checked on the basis of the said value (w).

2. Method according to claim 1, wherein the user blocks the said value (w) in the first step by issuing a derived value (w'') instead of the said value (w).

3. Method according to claim 2, wherein the blocking is carried out with the help of a one-way function (F) operating on the value (w).

4. Method according to claim 2 or 3, wherein the issuing of the value (w) in the first step (I) also comprises the making of a signature (σ).

5. Method according to any of the preceding claims, wherein the second step (II) is carried out at the request of the payment institution (B).

6. Method according to any of the preceding claims, wherein the first step (I) takes place during the charging with money of the payment means.

7. Method according to any of the preceding claims, wherein the first step (I) is carried out periodically.

8. Method according to any of the preceding claims, wherein, if a transaction is broken off prematurely, the second step (II) is used for detecting successful transactions.

9. Method according to claim 8, in which, for the execution of inter alia the second step, a special means is provided, such as a special card provided with an integrated circuit.

10. Method according to any of the preceding claims, wherein lost financial means are repaid to the user, if necessary.

11. Method according to any of the preceding claims, wherein the electronic payment means comprises a card provided with an integrated circuit.

12. Payment means provided with an integrated circuit, such as a so-called smart card, designed for tracing payment data in an anonymous payment system by issuing a value (w; w'') characterising the user's payment data to the payment institution (B), which value is stored by the payment institution, and, if tracing is desired, releasing said value (w), thus enabling a payment institution to check payment data on the basis of said value.

1/1

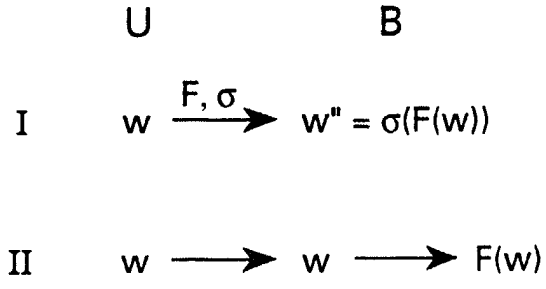

U
B
I
w
F, σ
w" = σ(F(w))
II
w
w
F(w)

Fig. 1

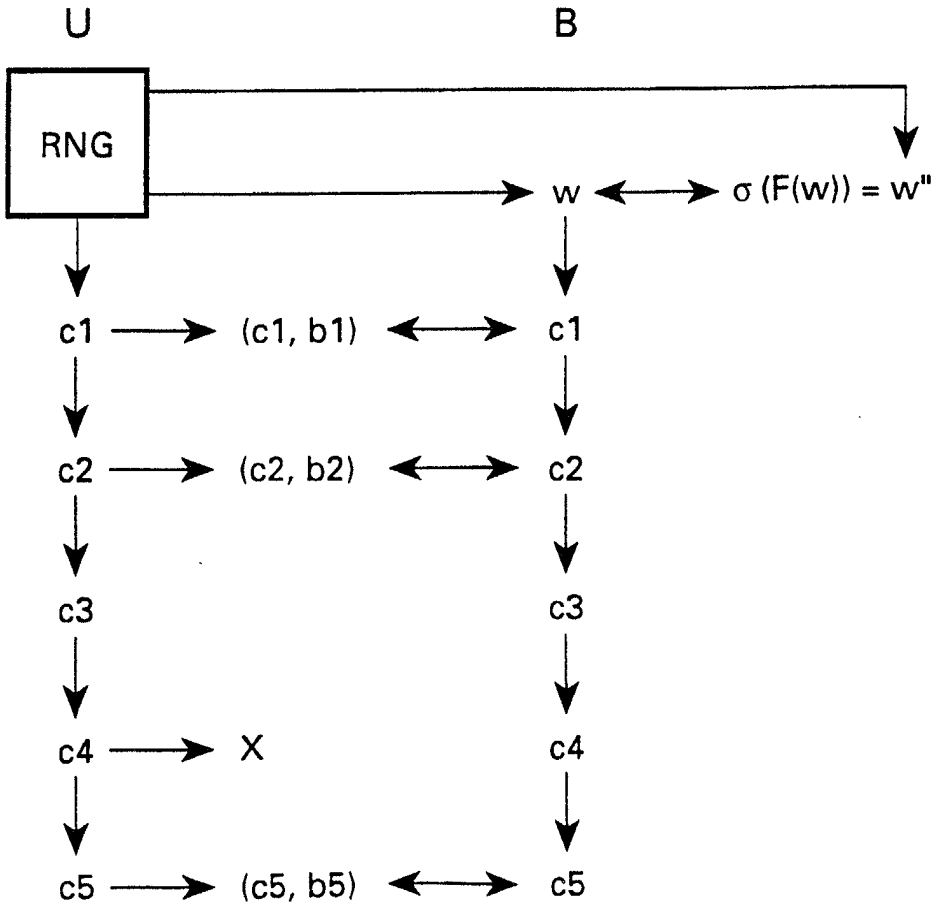

U
B
RNG
w
σ (F(w)) = w"
c1
(c1, b1)
c1
c2
(c2, b2)
c2
c3
c3
c4
X
c4
c5
(c5, b5)
c5

Fig. 2

INTEI .TIONAL SEARCH REPORT

Inten. ial Application No
PCT/EP 96/02997

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/08 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F G06F G07C H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,5 018 196 (K. TAKARAGI) 21 May 1991 cited in the application see abstract; figures 1-4 see column 3, line 63 - column 6, line 7 ---	1-6,8-11
A	EP,A,0 363 122 (FUJITSU) 11 April 1990 see abstract; claims 1-18; figures 1-5 see column 7, line 26 - column 9, line 8 ---	1,2,6, 11,12
A	WO,A,93 08545 (JONHIG) 29 April 1993 see abstract; claims 1-8; figure 3 see page 15, line 28 - page 18, line 24 --- -/--	1,11,12

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 November 1996	22. 11. 96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	**Authorized officer** David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTE[illegible]ATIONAL SEARCH REPORT

Inter[illegible]nal Application No
PCT/EP 96/02997

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,4 993 068 (G.V. PIOSENKA) 12 February 1991 cited in the application see abstract; figures 1-3B see column 5, line 28 - column 7, line 30	1-4,9, 11,12
A	DE,A,41 19 924 (SIEMENS) 24 December 1992	
A	US,A,5 420 926 (S.H. LOW) 30 May 1995	
A	DE,C,40 03 386 (SIEMENS) 23 May 1991	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTEI TIONAL SEARCH REPORT

...iformation on patent family members

Inter nal Application No
PCT/EP 96/02997

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-5018196	21-05-91	JP-B- 8027812	21-03-96
		JP-A- 62254543	06-11-87
		JP-A- 62056043	11-03-87
		JP-A- 2170184	29-06-90
		US-A- 4885777	05-12-89
		DE-A- 3687934	15-04-93
		EP-A- 0214609	18-03-87
EP-A-0363122	11-04-90	JP-A- 2096872	09-04-90
		JP-B- 6022030	23-03-94
		CA-A- 1319432	22-06-93
		DE-D- 68920107	02-02-95
		DE-T- 68920107	11-05-95
		US-A- 5097115	17-03-92
WO-A-9308545	29-04-93	AU-B- 663739	19-10-95
		AU-A- 2888692	21-05-93
		BR-A- 9205416	17-05-94
		CA-A- 2098481	17-04-93
		EP-A- 0567610	03-11-93
		JP-T- 6503913	28-04-94
		PL-A- 299825	18-04-94
		US-A- 5440634	08-08-95
US-A-4993068	12-02-91	NONE	
DE-A-4119924	24-12-92	NONE	
US-A-5420926	30-05-95	CA-A- 2134133	06-07-95
		EP-A- 0662673	12-07-95
		JP-A- 7234904	05-09-95
DE-C-4003386	23-05-91	AT-T- 129369	15-11-95
		DE-D- 59009799	23-11-95
		EP-A- 0440914	14-08-91
		ES-T- 2077621	01-12-95
		US-A- 5208858	04-05-93